

McAfee Security for Email Servers

Надежная защита содержимого для серверов Microsoft Exchange и Lotus Domino

Для защиты вашей электронной почты McAfee объединяет средства проверки содержимого, анализа репутации и защиты от вредоносных программ. Мы предлагаем несколько слоев защиты и вариантов развертывания, включая пограничный транспортный сервер на периметре сети, транспортный сервер-концентратор и почтовый сервер.

Ключевые преимущества

- **Постоянная доступность и работоспособность ваших систем.** Предотвращайте проникновение вирусов и червей через электронную почту и их распространение внутри ваших систем через серверы Microsoft Exchange и Lotus Domino.
- **Поддержание уровня производительности труда ваших сотрудников.** Блокируйте нежелательные сообщения и фишинговые атаки.
- **Управление через единую консоль.** Программное обеспечение McAfee ePO предоставляет мощную единую консоль управления, обеспечивающую контроль и администрирование систем, а также функцию просмотра отчетов.
- **Защита критически важных данных.** Выполняйте фильтрацию входящих и исходящих сообщений, направленную на защиту информации и снижение уровня корпоративной ответственности с помощью технологий защиты от утечки данных (DLP) и оценки репутаций IP-адресов, сообщений и файлов.
- **Интуитивно понятный графический пользовательский интерфейс.** Удобный интерфейс обеспечивает подробные отчеты, таблицы, а также статистику почтового трафика, получаемую в режиме реального времени.

McAfee® Security for Email Servers обнаруживает и выполняет фильтрацию вирусов, червей, троянов и иных потенциально нежелательных программ. Решение совместимо с серверами Microsoft Exchange и Lotus Domino, блокирует нежелательную почту и выполняет фильтрацию сообщений для защиты от проникновения в вашу сеть информации неподобающего характера и предотвращения утечки конфиденциальных данных, помогая обеспечивать соответствие политикам и нормативно-правовым требованиям.

Решение McAfee Security for Email Servers обеспечивает многослойную защиту входящих и исходящих сообщений, начиная со сканирования сообщений на наличие вредоносных программ по запросу, до принудительного применения политик с целью предотвращения утечки данных или несанкционированного использования конфиденциальной информации.

- **Лучшая в отрасли защита.** Решение использует передовые технологии McAfee для сканирования в памяти и добавочного сканирования по запросу, позволяющие удалять вирусы, черви, трояны, а также иные угрозы, относящиеся к входящей и исходящей электронной корреспонденции.
- **Мощная внутренняя защита.** Обнаруживает угрозы, способные проникать сквозь защиту периметра или попадать в сеть через зараженные ноутбуки и внутреннюю электронную почту. Решение также блокирует нежелательную почту с помощью модуля защиты от нежелательных сообщений.
- **Мощные средства фильтрации содержимого.** Решение обеспечивает применение корпоративных политик защиты электронной почты с помощью фильтрации запрещенных типов файлов, содержимого оскорбительного характера и блокирования каналов утечки конфиденциальной информации.
- **Управление через единую консоль.** В решении используется платформа McAfee ePolicy Orchestrator® (McAfee ePO™) для развертывания, управления системой безопасностью и просмотра подробных графических отчетов.

Многослойная защита электронной почты Комплексная защита от вредоносных программ

Решение McAfee Security for Email Servers базируется на программном обеспечении защиты от вредоносных программ, которое выполняет оценку репутаций и работает в режиме реального времени, что значительно снижает уязвимость к новым угрозам. Используя «облачную» технологию McAfee Global Threat Intelligence™ (McAfee GTI™), решение McAfee направляет отпечаток любого подозрительного файла в лабораторию McAfee Labs, где выполняется мгновенный анализ репутации. Если отпечаток будет распознан как известная вредоносная программа, то соответствующий ответ для блокирования файла или помещения его в карантин последует в течение миллисекунд. Технология оценки репутации электронной почты с помощью технологии

McAfee GTI — наш комплексный облачный сервис, который в реальном времени анализирует репутацию электронных сообщений и их отправителей. Благодаря этому сервису продукты McAfee могут защитить клиентов от известных и новых угроз, исходящих от электронных сообщений, в том числе от спама.

Репутация сообщений

Для оценки вероятности вредоносного характера сообщения решение применяет технологию анализа репутации электронных сообщений, а также такие факторы, как шаблоны рассылки нежелательных сообщений и поведение IP-адресов. Получаемый рейтинг основан не только на совокупной информации датчиков, направляющих запрос в «облако» McAfee, и на анализе, выполненном в лаборатории McAfee Labs, но также на корреляции информации о различных угрозах, включая веб-трафик, электронную почту и сети.

Репутация IP-адресов

Используя IP-адрес передающего сервера, решение обнаруживает угрозы, содержащиеся в электронных сообщениях. Оценка репутации IP-адресов предотвращает ущерб и хищение данных благодаря блокированию электронных сообщений у шлюза.

Круглосуточная защита ваших серверов

Проверка входящих и исходящих сообщений электронной почты на наличие вирусов, червей, троянов и иных вредоносных программ. Кроме того, вы можете сканировать всю внутреннюю электронную корреспонденцию, чтобы заблокировать червей и предотвратить их распространение внутри системы. McAfee Security for Email Servers автоматически загружает самые последние антивирусные базы (DAT-файлов) через HTTP, FTP, общий доступ к файлу в сети или централизованную консоль управления McAfee ePO.

Обеспечение нормативно-правового соответствия

Фильтрация сообщений по их размеру, содержанию и содержанию вложений. Блокирование или помещение в карантин сообщений, содержащих контролируемое содержимое в теме сообщения, в тексте письма или в приложениях.

Экономия времени и ресурсов

Встроенные фильтры содержимого упрощают создание политик и их принудительное применение. Создание глобальных правил с исключениями, необходимыми для отдельных сотрудников и структурных подразделений. Управление через встроенный HTML-интерфейс или платформу McAfee ePO.

Спецификации

Объем электронной почты и совместно используемых данных, находящийся на почтовых серверах, растет в геометрической прогрессии. Решение McAfee Security for Email Servers поддерживает среды Microsoft Exchange и Lotus Domino, обеспечивая продуктивную работу сотрудников, а также работоспособность и доступность систем в режиме 24/7.

Требования для установки решения McAfee Security for Microsoft Exchange

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Требования к серверу Microsoft Exchange

- Exchange Server 2003, включая 32-разрядную версию
- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013
- Поддерживаются серверы Exchange с кластером

Требования для установки решения McAfee Security for Lotus Domino на Windows

- Microsoft Windows Server 2008 и 2008 R2
- Поддерживаемые версии Lotus Domino: 8.5.x (32- и 64-разрядные версии)

Требования для установки решения McAfee Security for Lotus Domino на Linux

- Novell SUSE Linux Enterprise Server (SLES) 10 и 11
- Red Hat Enterprise Linux (RHEL) 5.x и 6.x
- Lotus Domino 8.5 (32- и 64-разрядные версии)

Фильтрация содержимого

Сканирование содержимого и текста в строке темы, в тексте электронного сообщения и вложения. Создание ваших собственных правил фильтрации содержимого на основе регулярных выражений (Regex).

Предотвращение утечки данных и обеспечение нормативно-правового соответствия

Механизмы предотвращения утечки данных (DLP) обеспечивают соответствие отправленных (находящихся в процессе отправки) или хранимых электронных сообщений политикам и правилам защиты конфиденциальной информации, принятым в вашей организации, а также нормативно-правовым требованиям. Встроенные словари, которые включают правила обеспечения нормативно-правового соответствия, специфические для каждой компании и каждой страны, обеспечивают быструю настройку фильтров содержимого. Встроенный бизнес-процесс автоматически направляет электронные сообщения, помещенные в карантин, на аудиторскую проверку.

Фильтрация нежелательной почты и повышение производительности

Модуль защиты от нежелательной почты позволяет отфильтровать нежелательные и фишинговые электронные сообщения, способствуя поддержанию производительности сотрудников и экономии дискового пространства на серверах электронной почты. Пользователи могут составлять свои собственные «белые» и «черные» списки. Концепция единого карантина, используемого совместно с решениями McAfee для защиты шлюзов, позволяет пользователям без труда получить доступ к единому карантину.

Уведомления о техническом состоянии продукта
McAfee Security for Email Servers направляет уведомления о состоянии продукта конкретному администратору. Настройка системы и графиков отправки уведомлений выполняется в соответствии с вашими требованиями.

Установка обновлений без труда

С помощью автоматической рассылки обновлений вы всегда будете получать самые последние данные об угрозах от McAfee Labs, крупнейшего в мире центра исследований угроз.

Централизация и консолидация карантин для вашей электронной почты

Диспетчер McAfee Quarantine Manager, включенный в решение McAfee Security for Email Servers, объединяет в едином решении функции помещения в карантин и управления программами защиты от нежелательной почты. Диспетчер McAfee Quarantine Manager удобен в управлении, позволяет направлять образцы угроз в McAfee Labs. Решение обеспечивает детальный административный контроль, автоматическую синхронизацию пользователей через серверы LDAP, управление пользователями или глобальными «черными» и «белыми» списками, а также формирование настраиваемых отчетов. Управление всеми этими операциями выполняется с помощью платформы McAfee ePO.

Поддержка всех ваших серверов

Поддержка всех ваших почтовых серверов большинством операционных систем, включая Microsoft Windows и Linux, как на 32-разрядных так и 64-разрядных платформах.

Сканирование и защита хранилищ электронной почты

McAfee Security for Email Servers поддерживает функции планового сканирования по запросу, а также функции выборочной настройки, что позволяет выполнить сканирование быстрее, чем с помощью традиционного метода полного сканирования. Например, решение позволяет выполнить сканирование только электронных писем с приложениями или непрочитанных писем. Кроме того, вы можете сканировать сообщения по темам, отправителям, получателям, получателям копий писем, кодам сообщений. Далее можно установить настройки для сканирования писем, полученных в течение определенного периода времени или имеющих определенный размер.

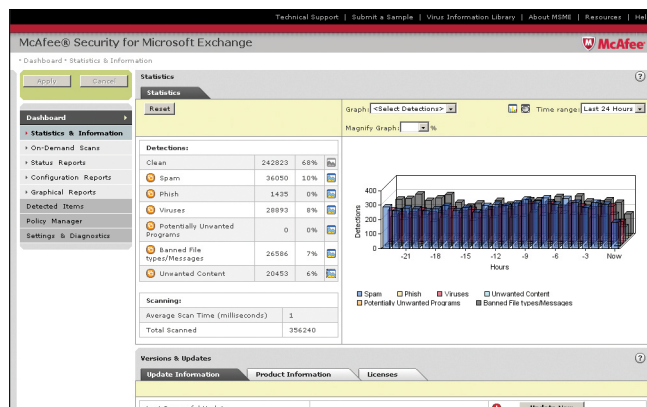


Рис. 1. Удобный интерфейс обеспечивает подробные отчеты, таблицы, а также статистику почтового трафика, получаемую в режиме реального времени.



ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

McAfee, логотип McAfee, McAfee ePolicy Orchestrator, McAfee ePO, McAfee Global Threat Intelligence и McAfee GTI являются товарными знаками или зарегистрированными товарными знаками корпорации McAfee, Inc. или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Планы выпуска продуктов, спецификации и описания, приведенные в настоящем документе, предоставляются только в информационных целях и могут подвергаться изменениям без предварительного извещения; они поставляются без предоставления гарантии какого-либо вида, явной или подразумеваемой. Copyright © 2013 McAfee, Inc. 60079ds_security-email-servers_0213_fnl_ASD